TMA Privacy Office Information Paper

Records Management◆FOIA◆DUAs◆HIPAA Compliance◆ADP Security◆Privacy Act◆System of Records◆PIAs

Information Access Management

HIPAA Security◆November 2003

Standard Requirement

Covered entities are required to implement an information access management plan as part of their administrative safeguards. This plan should include policies and procedures for authorizing access to electronic protected health information (EPHI). It also must determine who may access what types of health information. While this access is not based on worker roles, this rule does require differentiating information access given to different categories of workers. This differentiation depends on the covered entity's risk analysis, size, structure and business needs. This means that a covered entity would first establish a set of policies that lists and describes the different categories of workers; second, determine the types of information needed by each of those categories of workers; and third, establish the permitted uses (read, write, amend) of each type of information for each category. Each worker should only have access to the minimum amount of information needed to achieve the purpose of its use. Included in this plan should be policies and procedures that describe how each worker is given access to information, determine who has the authority to assign categories and the level of access given to that category, and finally, determine the process for setting up accounts, including how to make changes to existing accounts. A corresponding set of policies and procedures should include periodic reviews of the accounts to ensure that they are current and accurate.

This standard has three implementation specifications, with the first being required and the following two being addressable.

- isolation of any health clearinghouse functions,
- access authorization, and
- access establishment and modification.

Implementation Specifications

The first specification takes steps to protect its EPHI from unauthorized access by a larger organization. In some cases a clearinghouse may be part of a larger organization that has functions that do not relate to the clearinghouse. These functions could include receiving, formatting, and transferring health data. In this type of situation, the clearinghouse must implement policies and procedures that protect the EPHI in the clearinghouse from outside persons who are not authorized to access the information. This notion of putting up barriers inside the clearinghouse is similar to the barriers that must be erected within hybrid entities under the Privacy Rule. The health care component of the Privacy Rule is now paralleled in the Security Rule. This segregation requirement is also imposed on any kind of covered entity. (See discussion in the Final Rule pp.8334, 8358) MHS does not currently include a clearinghouse so this implementation specification does not apply at this time. It does contract with companies with clearinghouse functionality. These companies are covered entities in their own right.

TMA Privacy Office Information Paper

Records Management • FOIA • DUAs • HIPAA Compliance • ADP Security • Privacy Act • System of Records • PIAs

Information Access Management

HIPAA Security • November 2003

The second and third specifications are both addressable. In the second specification, covered entities should implement policies and procedures for granting an individual access to EPHI. These should include what authorizations and clearances are needed before an account can be established. In the third specification, covered entities should implement policies and procedures that establish, document, review, and modify a user's right of access to a workstation, transaction, program or process. Once individuals receive appropriate authorization for access, the Information Technology (IT) Department must correctly enroll them into the system. The policies and procedures that are part of these two specifications are very similar to those of the workforce security standard. This redundancy reflects the importance of formal, documented policies and procedures that defines the level of access for personnel who are authorized to access electronic PHI, including how it is granted and modified. Like the workforce security standard, the policies and procedures falling under these specifications must be guided by the Privacy Rule's minimum necessary standard.

See also:
45 CFR 164.105, 164.308(a)(4), 164.314

Federal and DoD regulations that support this standard
DoD 8510.1-M
DoDD 8500.1
DoDI 8500.2